UBM

I 7 must dell'end-user computing per la forza lavoro che usa Windows 10

Gennaio 2017

Il sistema operativo di Microsoft offre nuove opportunità per garantire produttività e sicurezza ovunque e qui viene illustrato come sfruttarle appieno.

L'ambiente di lavoro è cambiato radicalmente. Ora si passa facilmente dal desktop al laptop e dal tablet allo smartphone mentre ci si sposta rapidamente tra reti e luoghi per tenere il passo con le richieste sempre più pressanti della vita privata e professionale. Si utilizzano inoltre numerose risorse digitali in continua evoluzione, in cui rientrano sia le applicazioni tradizionali che quelle basate su cloud. Infine, con l'avvento della distribuzione agile e continua, le app e i sistemi operativi richiedono aggiornamenti più frequenti.

Gli approcci tradizionali alla gestione dei desktop e dei dispositivi mobili (MDM) non sono più adatti a questo nuovo Digital Workplace. L'IT di un'azienda deve riuscire a cambiare radicalmente e rapidamente la gestione dell'accesso degli utenti alle risorse digitali, per poter offrire la stessa esperienza d'uso su tutti i dispositivi nonostante i sistemi operativi e le piattaforme siano in continua evoluzione.

Windows 10 consente all'IT di adottare la gestione unificata degli endpoint in grado di supportare con più efficacia il nuovo Digital Workplace.

L'incapacità di adattarsi alle nuove regole del lavoro digitale con l'adozione di un approccio totalmente unificato alla gestione degli endpoint causa necessariamente deficit di produttività, indebolimento della sicurezza, problemi di conformità, minore coinvolgimento dei dipendenti e un più basso ritorno degli investimenti in tecnologia.

Con l'avvento di Windows 10, l'IT può finalmente ridefinire il modo di allineare la gestione degli endpoint alle nuove modalità del lavoro digitale. In particolare, l'IT può adottare la gestione unificata degli endpoint (UEM), che porta le tradizionali pratiche sulle policy di gruppo al livello successivo grazie alle nuove funzionalità push e alla consapevolezza del contesto in grado di supportare con più efficacia il nuovo Digital Workplace.

I 7 must per la forza lavoro che usa Windows 10

Questi sette must possono aiutare l'IT a utilizzare al meglio il nuovo sistema operativo di Microsoft per soddisfare in modo più efficace le esigenze dell'azienda.

1. Unificare i sili di gestione di dispositivi mobili e desktop

Il concetto di gestione unificata degli endpoint si basa sull'eliminazione dei sili di gestione di dispositivi mobili e desktop. Da un punto di vista logico e funzionale, un endpoint è tale indipendentemente dal suo fattore di forma o dal tipo di connessione di rete utilizzata. Considerando che gli utenti hanno bisogno di portare a termine il loro lavoro, sia che si trovino in ufficio che altrove, ha senso adottare un approccio unificato che consenta loro di accedere alle applicazioni e alle risorse necessarie su tutti i dispositivi.

In quest'ottica, vi sono diversi sviluppi tecnologici di recente concezione che favoriscono l'adozione di tale approccio unificato. Il primo è l'introduzione delle API MDM come nuovo standard per la gestione del sistema operativo. Con queste API, l'IT può passare dalla gestione tradizionale basata su oggetti Criteri di gruppo (GPO), che era essenzialmente adatta ai dispositivi in un dominio con connessioni di rete fisse, al modello mobile-cloud, applicabile a molteplici piattaforme e senza vincoli di rete e di dominio. Il secondo è l'introduzione di un set unificato di API (parte delle applicazioni universali Windows 10), che consente di eseguire una singola base di codice da distribuire e gestire senza difficoltà su qualsiasi dispositivo Windows.

Sponsorizzato da

vmware airwatch

Comprendendo e sfruttando i vantaggi di queste nuove funzionalità di amministrazione di Windows 10, l'IT può gradualmente passare alla gestione unificata degli endpoint. Con il passaggio delle aziende a questo nuovo modello, l'IT avrà bisogno, almeno per qualche tempo, di poter integrare le moderne efficienze dell'UEM con le funzioni tradizionali di gestione dei PC, come supporto dei GPO, script e sequenza delle attività, packaging e distribuzione delle app Win32, dal cloud in base alle esigenze. Si ottiene così una situazione vincente sia per l'azienda sia per il team delle operation degli endpoint.

2. Ridefinire il processo di integrazione

Storicamente, l'IT ha sempre integrato nuovi dispositivi tramite un processo di imaging predefinito che utilizzava risorse IT e ritardava la distribuzione all'utente finale. Ma un'integrazione lenta non è più accettabile. Le aziende hanno bisogno che i nuovi dipendenti siano produttivi fin da subito. I Millennial si aspettano che l'IT offra per i PC lo stesso modello di servizio pronto all'uso disponibile per gli smartphone, ma l'IT ha molte mansioni da svolgere oltre a caricare immagini sui dispositivi.

Un repository per il recupero automatico dell'area di lavoro permette all'IT di aggiornare i "prodotti" per l'area di lavoro più velocemente, con maggiore frequenza e con migliore granularità.

Grazie all'affidabilità di un sistema operativo che garantisce la connessione sicura e immediata alla rete e consente quindi ai dispositivi di recuperare i binari, le impostazioni e le autorizzazioni appropriati over-the-air, Windows 10 offre un ambiente estremamente favorevole a un tipo di integrazione semplificata.

Per beneficiare di questo modello di integrazione più efficiente, l'IT deve ridefinire il suo approccio passando dall'imaging dei dispositivi al provisioning dell'area di lavoro. In genere, ciò implica creare una serie di modelli di Digital Workspace che gli utenti possono recuperare automaticamente in base all'identità, al ruolo, alla piattaforma e alla versione del sistema operativo e a vari altri criteri. Un repository per il recupero automatico dell'area di lavoro permette altresì all'IT di aggiornare nuovi "prodotti" per l'area di lavoro più velocemente, con maggiore frequenza e con migliore granularità rispetto al passato, riuscendo a rimanere al passo con i requisiti tecnici e aziendali in rapida evoluzione.

3. Definire in modo intelligente le policy per un'estensione immediata e automatizzata ovunque

La maggior parte delle organizzazioni IT non è stata capace di applicare un approccio interamente basato su policy alla gestione degli endpoint, principalmente perché gli attributi delle policy dovevano essere implementati in modo estremamente frammentato, ad esempio per autorizzare l'accesso a un'istanza di SharePoint qui, limitare il geofancing lì e così via. L'utilizzo delle policy è stato compromesso anche dal fatto che occorre molto tempo per distribuirle su numerosi dispositivi, dentro e fuori dalla rete aziendale, e dalla necessità di riavviare tali dispositivi per applicare policy nuove o modificate.

Per superare questi ostacoli, l'IT ha bisogno di implementare una reale gestione degli endpoint basata su policy che offra un punto di controllo unificato per tutti gli attributi, tramite la tecnologia MDM moderna, i GPO tradizionali o entrambi, ovunque. L'IT può così definire policy complete per l'accesso, l'autenticazione, la crittografia, i whitelist, i controlli di sessione basati sul contesto e molto altro su tutti i dispositivi Windows e i dispositivi che eseguono altri sistemi operativi (ad esempio, iOS, Android, macOS e altri), all'interno e al di fuori del perimetro aziendale. Il tutto con la sicurezza che tali impostazioni delle policy verranno applicate immediatamente.

4. Abilitare il self-service contestuale

Con la disponibilità di una gestione delle policy efficace, l'IT può passare in modo più aggressivo a un modello self-service che consente agli utenti di aggiungere le applicazioni e le risorse consentite ai propri Digital Workspace. Questo perché le policy assicurano che gli utenti non possano utilizzare senza autorizzazione applicazioni o risorse a cui non devono accedere.

L'IT deve favorire il self-service rendendo più semplice la creazione di portali di applicazioni che consentono agli utenti di accedere alle applicazioni consentite disponibili (come le app Win32 tradizionali e quelle nuove nel Windows Store, il software commerciale di terze parti, le applicazioni sviluppate internamente, le app SaaS e le applicazioni remote pubblicate) sulla base dell'identità, del ruolo e delle responsabilità, della posizione e così via. L'IT può anche creare delle policy per questi portali per salvaguardare la conformità delle licenze e ottimizzare al contempo l'utilizzo simultaneo tramite meccanismi di riciclo e recupero delle licenze.

Il risultato è un'esperienza d'uso maggiormente di tipo consumer, che consente ai dipendenti di essere più produttivi riducendo i carichi di lavoro amministrativi dell'IT.

5. Gestire gli aggiornamenti del sistema operativo senza lo stress del "Patch Tuesday"

Una soluzione per la gestione unificata degli endpoint che supporta gli aggiornamenti granulari del sistema operativo su tutti i dispositivi e le reti assicura l'uniformità degli endpoint senza compromettere la produttività degli utenti.

È importante sia per la sicurezza che per l'assistenza assicurarsi che il sistema operativo degli endpoint sia sempre aggiornato. Tuttavia, il tradizionale modello di installazione degli aggiornamenti in blocco causa interruzioni e risulta inefficiente, oltre a limitare la frequenza con cui l'IT esegue gli aggiornamenti, creando ampie finestre di vulnerabilità e ritardando l'implementazione di nuove funzionalità del sistema operativo.

Grazie alla migrazione delle aziende a Windows 10, l'IT può ora controllare la cadenza degli aggiornamenti definendo in modo più flessibile le policy per la loro esecuzione. Gli aggiornamenti delle funzionalità possono essere distribuiti immediatamente insieme agli aggiornamenti cruciali per la sicurezza ("Current Branch"), con un breve ritardo per consentire il test pre-distribuzione ("Current Branch for Business") oppure al momento deciso dall'IT ("Long-Term Servicing Branch") per le distribuzioni più delicate, come sistemi medici e finanziari.

Nonostante Windows 10 semplifichi il problema dell'applicazione delle patch in blocco rendendo possibili gli aggiornamenti continui over-the-air, l'IT necessita comunque di una soluzione per la gestione unificata degli endpoint che supporti gli aggiornamenti granulari del sistema operativo su tutti i dispositivi, ovunque e su qualsiasi rete, non appena diventano disponibili. Ciò assicura l'uniformità degli endpoint senza compromettere la produttività degli utenti e riduce al minimo le vulnerabilità per la sicurezza eliminando i ritardi nell'implementazione delle correzioni dei problemi critici.

6. Ottimizzare l'automazione delle policy e i report per semplificare la conformità

Con la sempre maggiore complessità dell'ambiente aziendale, la conformità è diventata un problema per l'IT e il tutto è reso più complicato dall'utilizzo di processi manuali non monitorabili e da strumenti di gestione degli endpoint che producono report frammentati.

La gestione unificata degli endpoint allevia questa situazione in vari modi. Il primo è la capacità di offrire un meccanismo automatizzato e centralizzato per definire e applicare le policy di conformità ovunque. Il secondo è l'offerta di una visibilità unificata di tutti gli endpoint in modo che l'IT possa rilevare senza difficoltà e risolvere in modo automatico le anomalie correlate alla conformità in tali dispositivi.

Il terzo, ma spesso il più importante quando si verifica un audit di conformità, è la possibilità dell'IT di consolidare i report relativi alla conformità. L'unificazione dei report rende molto più semplice fornire agli auditor velocemente la documentazione che cercano e superare l'audit a pieni voti. I report unificati sono in genere considerati molto più credibili dagli auditor, perché eliminano i molteplici passaggi per il consolidamento dei dati, una procedura che può introdurre errori e inesattezze nella documentazione di conformità.

7. Determinare funzionalità per la privacy che consentano l'utilizzo misto dei dispositivi, per lavoro e per uso personale

L'IT delle aziende deve fare i conti con l'ormai diffuso utilizzo dei dispositivi mobili sia per lavoro e che per piacere. Per gestire questa situazione occorre adottare un programma BYOD ufficialmente riconosciuto che fissi le linee guida per l'utilizzo personale dei dispositivi aziendali o per una qualsiasi combinazione di uso privato e aziendale. Tuttavia, qualsivoglia approccio misto richiede l'astrazione sicura del Digital Workspace del dipendente dall'hardware sottostante.

Windows 10 semplifica questa astrazione tramite la containerizzazione delle app, dei contenuti e della connettività relativi all'ambiente di lavoro. Il sistema operativo è in grado di identificare i contenuti aziendali sulla base di attributi come il file server di origine, il server di posta, l'indirizzo IP e l'indirizzo DNS. I contenuti possono quindi essere posizionati automaticamente nel proprio container di riferimento e crittografati senza interrompere l'esperienza d'uso. Ciò consente di applicare policy e azioni di amministrazione, come le cancellazioni in remoto, ai container aziendali senza coinvolgere i contenuti personali.

Tali funzionalità tecniche si rivelano estremamente preziose in un'epoca in cui il confine tra vita privata e vita professionale è sempre meno definito. La tutela della privacy è sempre più importante anche per l'elevato ricambio del personale e il crescente ricorso all'outsourcing, che interessano la governance dei dati e sono soggetti a normative che regolamentano gli obblighi datore di lavoro-dipendente, come la normativa generale sulla protezione dei dati dell'UE. Per risolvere in modo efficace questi problemi, l'IT deve definire e automatizzare adeguatamente tutti i parametri delle policy rilevanti.

Il valore dell'UEM

Vale la pena investire nella gestione unificata degli endpoint e nell'automazione delle policy. Il lavoro viene continuamente e radicalmente trasformato dalla tecnologia digitale, la quale è essa stessa radicalmente trasformata dalla mobility diffusa. Con l'adozione delle sette pratiche sopra descritte, le organizzazioni IT possono ottenere molti importanti vantaggi, tra cui:

- **Notevole riduzione delle attività di amministrazione degli endpoint.** Con budget e personale limitati, l'IT non è in grado di far fronte ai costi di proprietà degli endpoint che continuano a crescere senza controllo. La gestione UEM con Windows 10 consente di eliminare i tempi e le spese operative per gli endpoint e di dedicare le poche risorse disponibili ad altro.
- **Esperienza d'uso ottimizzata.** Quanto più velocemente l'IT è in grado di dare ai dipendenti quello che vogliono e che necessitano, più aumenta la loro produttività, e questa maggiore produttività si traduce direttamente in clienti più soddisfatti, più innovazione e migliori prestazioni aziendali.
- **Azienda più sicura.** Gli endpoint sono una grossa minaccia per l'azienda se non vengono gestiti in modo adeguato. I controlli unificati e opportunamente automatizzati degli endpoint riducono in modo considerevole i rischi per la sicurezza e la conformità senza compromettere la produttività.
- **Agilità aziendale superiore.** Le aziende non possono agire velocemente se la distribuzione delle funzionalità digitali agli utenti finali è lenta. Eliminando i punti di frizione dalla distribuzione digitale, l'UEM e Windows 10 offrono l'agilità necessaria.

È famoso il consiglio di Wayne Gretzky, mutuato dal padre, che recita di "pattinare nella direzione in cui sta andando il dischetto, non nella direzione in cui si trovava". Lo stesso vale per la gestione degli endpoint. L'IT deve guidare la trasformazione degli endpoint o ne subirà pesanti conseguenze, come costi più alti, violazioni più frequenti della sicurezza e una forza lavoro di Millennial frustrata. Se implementati e gestiti in modo corretto nel tempo, l'UEM e Windows 10 rappresentano un'alternativa estremamente interessante.